U.S. Department of Justice

REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE

Table of Contents

digital evidence on scene, subpoenas and search warrants can be obtained if the victim prefers. In either case, investigators are committed to working collaboratively with victims to minimize any disruption to business during an investigation.

After obtaining digital copies of any affected devices, investigators may then turn to other devices in the victim's architecture, including firewalls, log servers, and routers, to look for additional evidence of the perpetrator's presence. Investigators will also image these devices, as needed, and forensically examine them. Such devices often contain traces of a criminal's passage through the infrastructure on the way to the affected device. In particular, many devices maintain log files that show when, and from where, the device was accessed. In addition to preserving and copying digital evidence, investigators may interview employees (especially those tasked with responding to cyber threats or securing infrastructure), regular users of the affected systems, and management.

2. *Online Data Review and Reconnaissance*

After reviewing information obtained from a victim or other primary sources of information regarding a cyberattack, investigators frequently will review online data, which may be open source, to determine their next investigative steps. In undertaking these actions, as with all their actions, investigators are trained to act consistently with our Nation's rule of law principles, and with our society's foundational respect for civil rights and civil liberties.[2]

The first step in online reconnaissance often involves use of the Internet Corporation for Assigned Names and Numbers' WHOIS database.[3] WHOIS is a directory of all of the IP addresses and domains on the Internet. WHOIS records usually display the name and contact information of the registrar (the business that sold the IP address or domain). Investigators can use the contact information to send legal process to the registrar in order to discover more information about the registrant (the user of the IP address or domain). WHOIS often contains self-reported information about the registrant, as well. In addition, an investigator often can tell from WHOIS and related information where a website is being hosted or who is hosting the e-mail server for a website, either (or both) of which can provide additional avenues for investigation.

After consulting WHOIS, investigators often perform online reconnaissance of the identifiers they have collected. This reconnaissance includes web searches looking for whether the identifiers have been used elsewhere and searches of social media to determine whether the identifiers are related to any accounts.

3. *Searching Records from Online Providers*

Successful WHOIS searches and online reconnaissance often results in the identification of e-mail providers, social media companies, registrars, and web hosting and computer hosting companies that may control additional evidence about a subject or

Protection Regulation ("GDPR"), which went into effect on May 25, 2018.

Broadly speaking, the GDPR regulates how private companies and governments process, store, and transfer data concerning E.U. residents, including how such data and information is handled and transferred into and out of the E.U. Violators could be subject to fines up to 4% of their gross revenue worldwide or 20 million Euros, whichever is greater, creating a serious financial incentive for covered entities not to violate the new regulation. Exceptions written into the GDPR should ensure that it does not affect the ability of U.S. law enforcement to obtain evidence through MLATs. Also, law enforcement-to-law enforcement sharing is covered by a separate directive and is thus outside of the scope of the GDPR. Still, significant questions and uncertainties exist about the GDPR, which could negatively affect law enforcement, including by impeding information sharing.

For example, some interpret the GDPR to require that the publicly-available WHOIS system remove information about the registrants of Internet domain names from public access, thereby necessitating the building and maintenance of secured law enforcement portals to access that information. As described in Chapter 3, prosecutors and law enforcement agencies around the world use the WHOIS system thousands of times a day to investigate crimes ranging from botnets to online fraud. The registrant data in WHOIS can create crucial leads to targets' identities, locations, and other pieces of their criminal infrastructure. This data can also help identify additional victims. Due to the significant risk associated with noncompliance with the GDPR, however, the private organization responsible for maintaining WHOIS has decided to remove much of the registrant data from the publicly-available segments of the system while the organization works with stakeholders, including the Department, to develop a GDPR-compliant system.

This is only one example of how the GDPR may be interpreted to impede the ability of law enforcement authorities to obtain data critical for their authorized criminal and civil law enforcement activities. Uncertainty about the GDPR also has placed in question not only voluntary disclosures of information about criminal activity—*e.g.*, by their employees, contractors, or customers—to U.S. law enforcement agencies, but also may cause companies with a significant E.U. presence to become reluctant to comply even with disclosures required by legal process, such as warrants and subpoenas, for fear that such a disclosure would be in violation of the GDPR. Absent official guidance, companies with significant E.U. business may become reluctant to participate in mandatory data transfers to U.S. law enforcement and regulatory authorities, which would impede effective tax collection, limit the ability of agencies to stop anti-competitive business practices, impair the work of public health and safety agencies, and undermine the integrity of global banking, securities, and commodities markets. This could also undercut the Department's mitigation programs for businesses and individuals that wish to cooperate in areas such as fraud, bribery, money laundering, sanctions violations, and antitrust matters—programs that yield information